Deployment Planning for Information Systems

Version 1.0

1. Overview:

Information systems (ISs) are an integral part of the Army's operational warfighting support, and our reliance on ISs requires that they be treated similarly as another weapons system. Commanders shall include ISs in their deployment and redeployment plans in order to protect the information, the IS, and the networks to which they connect. Commanders must ensure that ISs are properly prepared, and the individuals responsible for the management and security of these ISs are properly resourced and trained. When deployed, information systems must arrive in theater prepared to support the Combatant Commander and quickly integrate into an existing infrastructure. Redeploying ISs returning from theater must be sanitized and reconfigured to support the installation's base architecture as required. No system will connect to a garrison environment until these security actions are completed and verified.

ISs must be maintained in a proactive state of readiness, whether deployed or in garrison. Updated security baselines, IAVM compliance, host-based security protections, and full accreditation are the minimal requirements.

References:

A. AR 25-2, Information Assurance (PARAs: 1-4c(1); 5-4) (URL LINK)
B. DoDI 8500.2, Information Assurance Implementation (URL LINK)
C. Army CIO/G6 Memorandum; SUB: Interim Policy for Information Systems Deployment and Redeployment Vulnerability Management, DTD 10 MAR 04,

2. Point(s) of Contact (POC):

NETC-EST-IA, Office of Information Assurance and Compliance (OIA&C)
Greg A. Weaver greg.weaver@us.army.mil 703-602-7421 (DSN 332)

CECOM POC for the Universal Purge Tool
Edward Baidy edward.baidy@us.army.mil 732-427-5540

NSA Customer Service Desk, Protective Technologies (301) 688-5861

ACERTCNO website: https://www.acert.1stiocmd.army.mil/tools/.

3. Description of Former State: No requirement to identify or configure computer systems as part of a deployment or redeployment operation.

4. Description of Changes Instituted: Minimum acceptable procedures for identifying and securing ISs as part of operational deployment and warfighting.

A. These BBP measures shall be considered for ISs in the following scenarios:

(1) Any IS that is/was connected to any Joint, Interagency, or Multinational environment.
(2) Any IS that is/was identified for deployment into an operational theater external to the generating force (sustaining base) Area of Responsibility (AOR) for any length of time.
(3) Any IS that is/was used in any exercise or deployment to support Army organizations or agencies external to the generating force (sustaining base) architecture.
(4) Any IS that departs/departed installation support or is/was connected to a non-trusted/unverified network as part of an operation, exercise, or travel.

B. Local evaluations of the vulnerabilities and risks and reconnection approval processes are required before reconnecting systems.

DEFENSE EXHIBIT I for identification
PAGE OFFERED:___ PAGE ADMITTED:___
PAGE___ of___ PAGES

Deployment Planning for Information Systems
Version 1.0

C. Commanders, DAAs and DOIMs (or DOIM equivalents), must establish a quarantine and re-introduction policy and implement procedures that addresses the risks of re-introducing ISs returning from deployments to reconnect to their supporting networks.

5. Description of End State: Deployment and redeployment plans shall include the requirements identified in AR 25-2, Information Assurance and this BBP as part of the operational mission to protect ISs and networks. These requirements should be stated in unit operations orders and other directives with command emphasis.

6. Description of Required Resources: Assessment and scanning, patch and configuration management, and anti-virus software packages are the minimal required tools in order to manage deploying and redeploying ISs effectively. Training of individuals in the skills necessary to accomplish security management actions is critical for success.

7. Description of Derived Benefits Resulting from Implementation: Minimum acceptable IA requirements and standards established to safeguard information and IS.

8. Administrative Requirements:

A. Deployment planning shall include the requirements identified in AR 25-2, Information Assurance. Every IS or device shall have the latest authorized and acceptable security configurations applied before storage or transit. As a minimum, this configuration shall include; system identification, newest authorized operating system and applications service packs and updates; identified IAVM fixes; updated anti-virus products and signature files; and updated management software used in the theater if known. The IS will be labeled with this information before storage for ease of identification upon arrival in theater. Deployment planning shall include a management plan for ensuring security and management updates are accomplished as necessary during deployment.

B. Redeployment planning shall incorporate the requirements identified in AR 25-2, Information Assurance. Every IS or device returning must be safeguarded to the level of information contained on the system. Implement data consolidation and preservation procedures for lessons learned, after action reports, or analysis as required. As a security consideration, purge or re-baseline ISs before storing for transit.

C. Before connection to the installation environment from a deployment, all ISs must be either: purged and rebuilt, or processed through an assessment and certification station or quarantine procedure that will certify the integrity of the IS as updated to the latest security baseline, with IAVM compliance, anti-virus and management configurations as minimums. Evaluate the presence of unauthorized software or applications on returning systems and rebuild those systems containing unauthorized, illegal, or highly vulnerable applications or services. Ideally, identify or remove all non-upgradeable or non-supportable ISs from the inventory at this point and purge and appropriately label ISs for final disposal.

D. SAs/NAs shall be trained on the tools used to maintain security compliance. Deployment planning shall include successfully mastering those skills necessary to enforce security configurations, vulnerability assessment scanning, remediation, and reporting, and network management or operations capabilities.

E. Definitions and acronyms can be found in the AR 25-2 Glossary.

9. Related BBPs:

Deployment Planning for Information Systems
Version 1.0

04-PE-O-0001: Reuse of Army Computer Hard Drives (URL LINK)
03-VI-O-0001: Classified Data Spillage Procedures (URL LINK)
04-EC-O-0004: Network Assessment Scanning (URL LINK)

10. Products:

A. Norton Ghost, Enterprise License: Enterprise license will be made available.
Refer to the Army Small Computing Website for details on status and availability.
https://ascp.monmouth.army.mil/scp/index.jsp
B. Approved scanning and assessment applications.
C. Universal Purge Tool (CECOM developed; see POC).
D. Tamper Evident Security Tape: NSA POC.

11. Description: Ideally, the following steps should be addressed based upon requirements of the Commander and the DAA. Exceptions and approvals should be documented as part of the deployment planning.

A. Pre-deployment procedures should be performed at a centralized location to ensure all IS are inventoried, documented, and prepared for deployment.

(1) SA/NA and IA personnel preparations:

(a) System and Network administrators should enroll and complete any required or appropriate training as is available on the IA Custom Learning path on Smartforce/Skillsoft.
(b) Suggested training includes:
i. Intrusion Detection and Response in Networked Environments.
ii. Operating Systems and File Security Issues (Appropriate OS module).
iii. Introduction to Security in a Networked Environment.
iv. Access control and Physical Security.
(c) Obtain all required system, program, approved vulnerability assessment, and IA tools required to support ISs.
(d) Identify requirements and train users on acceptable use, anti-virus, physical security and incident handling/response procedures.
(e) Create and provide boot, purging, sanitization, and management software for deploying systems and units.
(f) Obtain war-dialing software to be used to identify rogue modem connections.
(g) Obtain copies of forensic applications (i.e. Log Collector) from the Computer Crimes Investigative Unit (CCIU) for applicable IS from the ACERTCNO website.
(h) Plan and practice emergency recovery operations for IS.
(i) Plan and practice purge and rebuild operations for IS.
(j) SA/NA and IA training links:
i. https://ia.gordon.army.mil
ii. http://my.smartforce.com
iii. https://iatraining.us.army.mil/

(2) IS preparation:

(a) Create a pre-deployment asset database/spreadsheet for inventory of IS, external media, portable and other devices.
(b) Verify that current IS hardware can support any new OS/updates.

(c) Purge old drive(s) if never performed.
(d) Replace/destroy outdated/unsupportable IS or hardware.
(e) Determine asset value (i.e. MAC level).
(f) Revision levels.
(g) Maintenance agreements.
(h) Lease details.

(3) Establish baseline OS for workstations and servers:

(a) Install latest Army baselined OS. (Consideration must be given to impact of the newest OS on that of the theater approved and supported OS.)
(b) Install latest service pack (SP) and all OS security/hotfix patches for the approved baseline.
(c) Remove unnecessary services or disable embedded unauthorized hardware (i.e. wireless capabilities). Ensure wireless and IR capability cannot be re-initiated by the user when prohibited.
(d) Remove or disable sample, test configurations, and default accounts from OS installation (e.g. guest, administrator).
(e) Configure default security parameters (passwords; accounts; etc).
(f) Configure system and OS defaults for theater operations (e.g. time zone, account format, audit logging).
(g) Document any program managed (PM), legacy, un-patchable, non-compliant, or non-upgradeable systems required for deployment and devise a risk management plan to protect these systems.
(h) Create and secure system specific boot disks for emergency recovery operations.

(4) Install/update necessary applications:

(a) Office applications.
(b) Anti-virus application with most recent update.
(c) Security applications if used (e.g. IPSec, Tripwire).
(d) Management/ remote management applications used in theater/exercise.
(e) Host based firewall or IDS/IPS.
(f) Patch Management agent.
(g) Backup-recovery software.
(h) Authorized/licensed applications (WinZip, Adobe Acrobat, etc).
(i) CAC/PKI Reader Applications (if not included in baseline).
(j) Functional applications and data as required.

(5) Perform vulnerability assessment on OS image.

(6) Remediate identified vulnerabilities.

(7) Load imaged OS onto workstations/servers.

(8) For systems that are preloaded with data before deployment, incorporated tamper identification measures to reveal evidence of tampering, prior to storage or transit. Tamper-evident measures should be unique and non-replicable by end users or unauthorized personnel. Backup copies of information shall be prepared and shipped or managed separately for COOP measures in the event of catastrophic loss of the IS.

(9) Place pre-deployment certification label on external case IAW local policy or as shown in the sample below.

(10) Create and provide baseline back-up images/software for deploying systems.

(a) Original media inventory verification.
(b) Original media labeled and stored (SW).
(c) License restrictions (SW).
(d) License conformance verification.

(11) Update Asset and Vulnerability Tracking Repository (A&VTR) with deploying assets and theater reporting requirements.

B. In-theater IA requirements:

(1) Asset Management:

(a) Verify pre-deployment inventory database/spreadsheet and tamper evidence verification measures.
(b) Physical identification of each asset.
(c) Physical location map (HW).
(d) IP and Ethernet address (HW).
(e) Weekly asset verification.
(f) Network probes (scanning).
(g) Process for adding/moving/decommissioning HW and SW.
(h) Data and process to determine asset value (i.e. MAC level).
(i) Update A&VTR as required.

(2) Facilities Management:

(a) Power supply capacity and distribution.
(b) UPS.
(c) Air conditioning.
(d) Fire control and protection measures.
(e) Environmental failure monitoring and alerting.
(f) Physical security.
(g) Appropriate maintenance contracts for core equipment.
(h) Appropriate console (privilege) management.
(i) Data center layout and network topology maps.
(j) Host responsibility assignments.
(k) IP allocations register.
(l) Critical support documents.

(3) Network Management:

(a) Network management console implemented.
(b) Proactive monitoring of network health.
(c) Network management provides alerts of network outages or failures.
(d) Network devices use common protocol to report failures (SNMP).
(e) Procedure for addition, removal and movement of network devices.
(f) Procedure for allocation and recovery of network addresses.
(g) Accurate network register maintained.

(h) Tool to scan for network exceptions: duplicate addresses, illegal addresses.
(i) Tools for identifying and isolating network faults.
(j) Policy and requirements for network gateway implementation.
(k) Policy for remote access (i.e. modem) facilities.
(l) Procedures for severing/restricting gateway and modem connections in the event of a security incident.
(m) Procedures and tools in place to protect network from exterior networks (e.g. firewalls).
(n) Intrusion Detection System (IDS) to detect illegal traffic on internal network.
(o) Procedures and tools for monitoring for illegally connected gateways/modems.
(p) Weekly network security audits performed.
(q) Reporting procedures for network outages, incidents, or intrusions IAW AR 25-2.
(r) Share notification, administrative, and technical contact information with the Regional/Theater RCERT/TNOSC/RCIOs.

(4) Server Management:

(a) Account management standards.
(b) Product installation and configuration standards.
(c) Host configuration baseline.
(d) Centralized audit server where all system logs are maintained and reviewed.
(e) Weekly, well defined house cleaning (rolling and archiving logs).
(f) System backups.
(g) Centralized administration - tools direct results and errors to central monitoring.
(h) Key aliases defined.

(5) Software Management:

(a) Policy for software location, distribution, replication and currency.
(b) Mechanism to inventory installed software.
(c) Mechanism/tools to remove unauthorized software.
(d) Procedures for license management.

(6) Data Management:

(a) Well-defined data archiving policy and procedure.
(b) Random restores to verify backup media and procedure.
(c) Tools to scan for data integrity (e.g. Anti-Virus products).
(d) Availability management addresses Redundant Array of Independent Disks (RAID).
(e) High Assurance (HA) systems implemented where approved.

(7) Data Security:

(a) Well-defined and communicated information security policy.
(b) User responsibilities acceptance form and acceptable usage statements.
(c) Formal security procedures implemented and routinely evaluated.
(d) Defined information security coordination (e.g. intra-inter theater, cross services, cross-domain, multi-national, coalition, etc).
(e) Allocation of information security responsibilities.
(f) Process for receiving and evaluating vendor and CERT advisories.
(g) Process for reporting and investigating suspected security breaches.

(h) Security logs reviewed on a daily/weekly basis.
(i) Automated alerts defined.
(j) Audit trails enabled and reviewed.
(k) Regularly used security methodologies and tools.
(l) Virus control systems in place, enforced and updated.
(m) Security methodologies and tools reviewed weekly for currency and applicability.
(n) Independent review of information security architecture, controls and mechanisms.
(o) Audits of physical, network, host and data security.
(p) Incident investigation reports, assessments and action plans.
(q) Risk assessment and contingency planning standards in place.

C. Re-deployment/staging area: When possible, these procedures should be performed at a centralized location to ensure all IS are inventoried, documented, and prepared for re-deployment. The recommended acceptable procedures for redeploying systems shall be data consolidation, IS purging, and label overprint before transit while any remaining activities can be conducted at home-station. As an absolute minimum, no system shall be connected to a garrison or home-station network until the system(s) has been certified as free from malicious logic, made compliant to current Army standards, and a compliance verification scan has been completed and vulnerabilities remediated. Rebuild any IS that can be, before reintroduction to the network. IASOs are primarily responsible for this action.

(1) IS preparation:

(a) Inventory current ISs hardware/software.
(b) Compare to pre-deployment reference and resolve discrepancies.
(c) Identify centralized server/system for data/file consolidation efforts.
(d) Identify file formats to be consolidated/moved to server (e.g. .ppt, .pps, .doc, .txt, etc.). Executable files will be excluded unless specifically designed or implemented while deployed. Executable code will be maintained separately from all data repositories.
(e) Identify classification and security requirements of files or aggregated data. Treat unknown or unmarked data as potentially classified until excluded.
(f) Establish defined data archiving policy and procedures.
(g) Virus scan and compress (e.g. zip) all data files transferred to the server.
(h) Identify and label all outdated/unsupportable/unserviceable IS or hardware.

(2) Purge all workstations and servers for transit when operationally permitted. For systems that are identified in the management plan as exempt from being purged or rebuilt, incorporate tamper identification measures to reveal evidence of tampering, prior to storage or transit of ISs. Backup copies of information shall be prepared and shipped or managed separately for COOP measures in the event of catastrophic loss of the ISs.

(3) Rebuild IS workstations and servers if operationally permitted.

(a) Install latest available Army baseline OS or approved Gold Standard.
(b) Install latest service pack and OS security/hotfixes or patches.
(c) Remove un-necessary services.
(d) Remove sample, test configurations, and default accounts from OS installation.
(e) Configure default security parameters (e.g. passwords, accounts).
(f) Configure system and OS defaults for garrison operations (e.g. time zone, account format, audit logging).

(4) Install necessary applications:

(a) Office applications.
(b) Anti-virus application with recent update.
(c) Security applications if used (e.g. IPSec, Tripwire).
(d) Management application used in garrison (if returned to installation network).
(e) Host based firewall or IDS/IPS.
(f) Patch Management agent (if used).
(g) Backup-recovery software (if used).
(h) Authorized/licensed applications (WinZip, Adobe, etc).
(i) CAC/PKI Reader Applications (if not included in baseline).

(5) Perform vulnerability assessment on OS image vulnerabilities.

(6) Remediate identified vulnerabilities.

(7) Load imaged OS onto workstations/servers.

(8) Place re-deployment certification label on external case IAW local procedures or as shown in the sample below.

(9) IS and IT hardware obtained for mission support: IT/IS systems, devices or peripherals obtained while deployed or in a deployment status are prohibited from being installed on installation networks until appropriate certification and accreditation documentation is updated or CCB/CCM approval and signature by the DAA. While operationally functional and locally required during an exercise or deployment, these items present an undue and undocumented risk to any garrison environment.

Deployment Planning for Information Systems
Version 1.0

Sample Pre-deployment/Transit label:

XX Command; S-6
Computer Name:
MAC address:
Serial Number:
Server Y N Purpose
Make: Model:
OS: XP 2K Baseline: Y N Version:
Classification: S U
IAVA Compliance through IAVA:
PKI: Y N
A/V Version and signature Date:
Assigned Section:
Verified by:

Sample Re-deployment/Transit label with Purge Overprint:

XX Command; S-6
Computer Name:
MAC address:
Serial Number:
Server Purpose
Make: Model:
OS: XP 2K Baseline: Y N Version:
Classification: S U
IAVA Compliance through IAVA:
PKI: Y N
A/V Version and signature Date:
Section:
Verified by:

Purged with (insert method) mm/dd/yyyy

Deployment Planning for Information Systems
Version 1.0

Sample Re-deployment/Transit label with Rebuilt Overprint:

XX Command; S-6
Computer Name:
MAC address:
Serial Number:
Server Y N Purpose
Make: Model:
OS: XP 2K P Y N Ver:
Classification: S U
IAVA Compliance IAVA:
PKI: Y N
A/V Version and signature
Section:
Verified by:

Rebuilt OS
(insert OS)
mm/dd/yyyy

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

SEP 01 2005

NETC-EST-I

MEMORANDUM FOR All Army Activities

SUBJECT: Implementation of Information Assurance Best Business Practice (IA BBP)

As the Army Office of Information Assurance and Compliance Director the undersigned approves the listed OIA&C BBP to support the Army Information Assurance Program (AIAP). The BBP will be implemented throughout all information systems and networks as applicable, as the Army standard for IA implementation for the identified purpose.

05-EC-M-0001: Deployment Planning for Information Systems; Version 1.0

Stephen J. Lunko
COL, GS
Director, CIO/G6 Office of Information
Assurance and Compliance